Appendix 3

PacketSight

This Page Blank (uspto)

PacketSight

Information Source Module Guide

Notices

This publication and the features described in it are subject to change without notice. While reasonable precautions have been taken in the preparation of the text, XACCT Technologies (1997) Ltd. and its subsidiaries ("XACCT") assume no responsibility or liability for any errors or omissions relating to the information or recommendations contained in this publication. The XACCT software products (the "Products") described in this publication are furnished expressly subject to the XACCT End-user License Agreement (the "Agreement"), which may be modified from time to time, and may be used or copied only in accordance with the terms and conditions set forth in the Agreement. The Product or components thereof may be protected by one or more US patents, foreign patents, pending applications, or national and international copyright laws. The Agreement contains, inter alia, limitations of liability and limited warranties. Please refer to the Agreement prior to installing or using the Product. THE USE OF THE PRODUCT IS EXPRESSLY SUBJECT TO THE TERMS AND CONDITIONS OF THE AGREEMENT.

XACCT, XACCT*usage*, XACCT Detail Record (XDR) and the XACCT logo are trademarks or registered trademarks of XACCT Technologies (1997) Ltd. Cisco, Cisco IOS, and Cisco Systems are registered trademarks of Cisco Systems, Inc. All other products or services mentioned herein are trademarks or registered trademarks of their respective owners. The XACCT product includes software developed by the Cryptix Development Team (http://www.systemics.com/docs/cryptix/).

Copyright © 1997-2000 XACCT Technologies (1997) Ltd. All rights reserved.

Corporate Office

XACCT Technologies, Inc.
2900 Lakeside Drive
Santa-Clara, CA 95054
USA
Tel: 408-654-9900
Fax: 408-654-9904

URL: www.xacct.com

International Office

XACCT Technologies (1997) Ltd.
12 Hachilazon St.
Ramat Gan 52522
Israel
Tel: 972-3-6180040
Fax: 972-3-5799798

Email: info@xacct.com

October , 2000

V.1.09

Contents

How to Use This Guide

This guide contains instructions on installing and using thePacketSight Information Source Module (ISM). It should be used in conjunction with the *XACCTusage User Guide.* It assumes a basic understanding of XACCT*usage*™ and its configuration. It is intended to be used in conjunction with the *XACCTusage User Guide.*

Document Conventions

The following typographic conventions are used in this guide:

Typeface or Symbol	Meaning	Example
Italics	References, new terms, and placeholders.	For a more detailed description of how XACCT*usage* works, refer to Chapter 5 of the *XACCTusage User Guide.*
Bold	Names of menus, options, and command buttons.	From the **Type** list, select **PacketSight** and then click **Next**.

Overview

The PacketSight Information Source Module (ISM) is what XACCT*usage* uses to pull usage and QoS information from XACCTpacketSight. XACCTpacketSight retrieves information from network interface groups allowing you to collect statistical information about the hardware interfaces of a device as well as data about the traffic that passes through each interface. For additional information on XACCTpacketSight please refer to the *XACCTpacketSight User Guide*.

The PacketSight ISM is a Data Collection Module (DCM). The PacketSight ISM collects information, processes it, and relays it to its associated Gatherer for further enhancement and storage. It serves as the trigger for Enhancement Procedures and initiates the flow of data through XACCT*usage*.

The PacketSight ISM returns information for over 60 data fields. This enables you to track general information, such as Client and Server IP addresses, HTTP Response Time, and URL Domain names.

Connecting With XACCT*usage*

The PacketSight ISM uses XACCTpacketSight as its Information Source. XACCTpacketSight reads packets from the network. The PacketSight ISM polls XACCTpacketSight in regular intervals to collect data. The PacketSight ISM converts the data into a Unified Network Information Record (UNIR). The UNIR is then pulled into XACCT*usage* by the Gatherer.

The Gatherer can then process and forward the UNIR to either of the following:

- Data Processing Module (DPM)
- Central Event Manager (CEM)

Examples of a DPM are the Aggregator ISM and Session ISM. The Aggregator ISM reduces the amount of data flowing through the system by outputting only the most relevant information determined by you. The Session ISM tags flows with identifiers (ID) to determine the duration of site visits.

Features of the PacketSight ISM

This section summarizes some of the features of the PacketSight ISM.

Note: To start using the PacketSight ISM, you must install the software on the CEM host and then configure the ISM.

The PacketSight ISM provides you with these features:

- **Automated interface selection**. You do not have to add the interfaces from which you want the ISM to collect data when you configure the ISM. The ISM will monitor all the interfaces that are specified by XACCTpacketSight. This is convenient because it saves you the time and effort of adding interfaces manually. In addition to this, if new interfaces are added to the device, the ISM will automatically start monitoring them, eliminating the need for reconfiguring it.
- **A rich array of output fields**. The PacketSight ISM has many output fields allowing you to collect a rich array of data, including data such as **Client IP**, **URL Domain**, and many others. See the section "PacketSight ISM Output Fields" for a complete list.

Information Source Setup

XACCTpacketSight must be installed and reading from the network interface group. For instructions on how to install and configure XACCTpacketSight, please refer to the *XACCTpacketSight User Guide.*

System Requirements

You can install the PacketSight ISM on all platforms on which you can install any XACCT*usage* components. See Chapter 2, "Preparing To Install XACCT*usage*," in the *XACCTusage User Guide* for a complete list.

Installing the PacketSight ISM

You can install the PacketSight ISM on all platforms on which you can install any system components. You install the ISM on the Central Event Manager (CEM) host using the basic procedure for installing Information Source Modules.

To run the PacketSight Information Source Module (ISM) installation program, you need root user access rights for the host on which the Central Event Manager is installed.

To run the Module installation program

1. Log in as root user.
2. Copy the PacketSight.tar.Z file from the CD-ROM to your /tmp directory.
3. Enter `cd /tmp` to change to your `tmp` directory.
4. Extract the files from the compressed distribution file by executing the following command:

   ```
   zcat PacketSight.tar.Z | tar xvf -
   ```

5. Execute the following command:

   ```
   ./xacct_upgrade
   ```

   The XACCT*usage* installation program starts. The program runs automatically informing you of the actions performed and asking you to confirm and select options.
6. When prompted to read the End-user License Agreement, press Enter to display the text.
7. Read the End-user License Agreement.

8 Do one of the following:

- Type y and press Enter, if you agree with the terms of the End-user License Agreement. The installation program proceeds to the next step.
- Type n and press Enter, if you do not agree with the terms of the End-user License Agreement. The installation program shuts down.

If you accepted the terms of the End-user License Agreement, the list of components you can install displays.

```
========================================================
            XACCTusage Module Installation
========================================================
You may choose components that will not be installed, by
selecting their number or you can press c to continue, q to
quit


   Install   Name              Description
   =======   ====              ===========
 1 Yes       PacketSight

Your selection :    c
```

9 Select the components you want to install following the instructions on your screen. Use the following procedures to enter your selection.

- To change the installation status of a system component on the list (to alternate between Yes and No), type the number of the component and press Enter.
- To continue with installation, type c and press Enter. The components selected to be installed (marked with Yes) will be installed.
- To quit the installation program, type q and press Enter.

The selected components are installed. If installation is successful, the Central Event Manager sends the modules you have installed to the appropriate host or hosts. If installation is not successful, you get a notification with a description of the problem.

Adding a PacketSight ISM to the XACCT*usage* Configuration

In order to use the PacketSight ISM, you must add an instance of it, that is a PacketSight IS, to the system configuration. You add the PacketSight IS to its associated Gatherer.

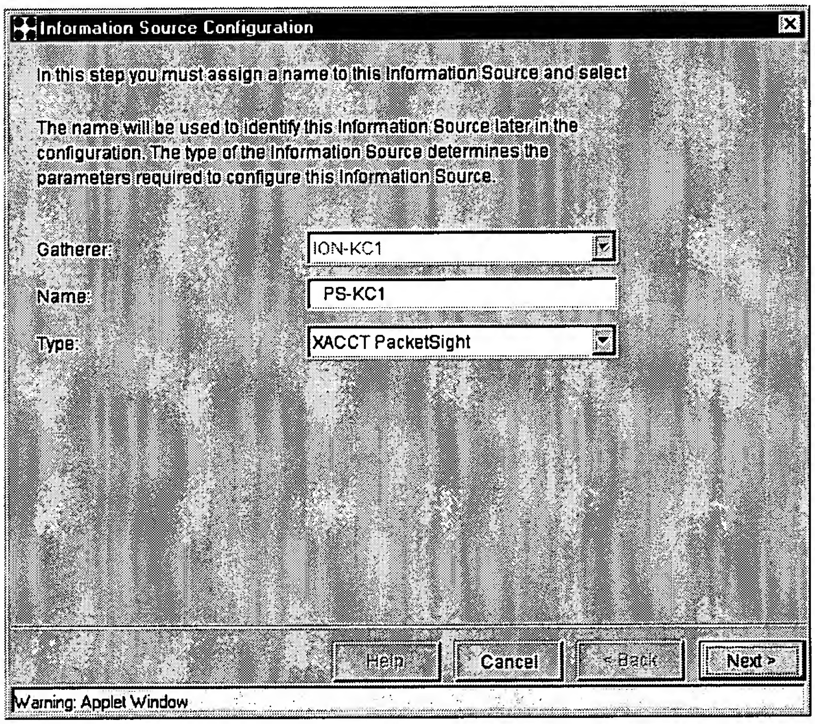
To add the PacketSight IS, you need the following:

- Administrator or Manager access rights to the system.
- License to use the PacketSight Information Source Module installed. (See the section "Installing Licenses" in the *XACCTusage User Guide* for details.)
- The Gatherer that the PacketSight ISM will be associated with, configured in the system.

To add the PacketSight Information Source using the shortcut menu

1 In the XACCT*usage* tree, right-click the Gatherer to which you want to add the PacketSight Information Source, and then click **New Information Source**. The Information Source Configuration wizard is displayed.

2 In the **Name** box, type a unique name for this Information Source.



In this step you must assign a name to this Information Source and select

The name will be used to identify this Information Source later in the configuration. The type of the Information Source determines the parameters required to configure this Information Source.

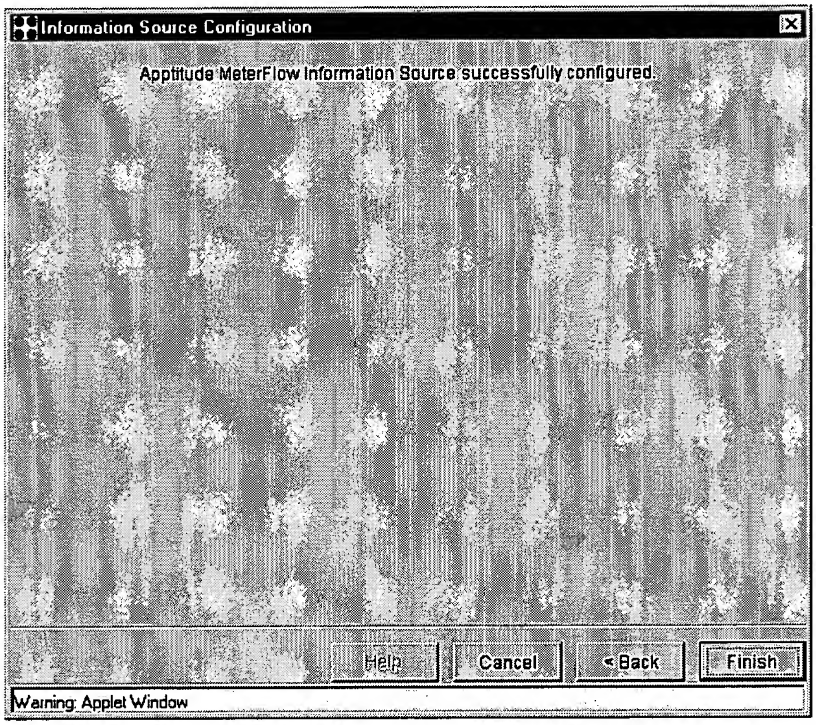
Gatherer: ION-KC1

Name: PS-KC1

Type: XACCT PacketSight

3 From the **Type** list, select **XACCT PacketSight.**

4 Click **Next**. A screen appears confirming that configuration of the information module has been successful. This may take a minute or two as the ISM is now being downloaded to the Gatherer.



Information Source Configuration

Apptitude MeterFlow Information Source successfully configured.

5 Click **Finish** to complete the procedure.

PacketSight ISM Output Fields

The PacketSight ISM provides the following output fields.

Field	**Description**
MF Client IP Address	The IP that was assigned to the user for dialup or or the permanent IP for the client.
MF Server IP Address	IP address of server sending data.
MF Service	The name of the protocol.
MF Client To Server Packets	Traffic packet count from client to server.
MF Server To Client Packets	Traffic packet count from server to client.
MF Client To Server Octets	Volume of traffic measured for a given application between two communicating end points, from the client to server.
MF Server To Client Octets	Volume of traffic measured for a given application between two communicating end points, from the server to client.
MF HTTP Response Code	Status code returned by web servers when a web page is requested.
MF Flow ID	A unique ID for a "flow".
MF Parent Flow ID	A unique ID for a parent "flow".
MF CS ERT SS N	Exchange Response Time, the n metric for exchange response time start to start from client to server.
MF CS ERT SS Sum X	Exchange Response Time, the summation X metric for exchange response time start to start from client to server.
MF SC ERT SS N	Exchange Response Time, the n metric for exchange response time start to start from server to client.
MF SC ERT SS Sum X	Exchange Response Time, the summation X metric for exchange response time start to start from server to client.
MF CS ERT SE N	Exchange Response Time, the n metric for exchange response time start to end from client to server.

Field	Description
MF CS ERT SE Sum X	Exchange Response Time, the summation X metric for exchange response time start to end from client to server.
MF SC ERT SE N	Exchange Response Time, the n metric for exchange response time start to end from server to client.
MF SC ERT SE Sum X	Exchange Response Time, the summation X metric for exchange response time start to end from server to client.
MF CS ART SS N	Application response time, the n metric for exchange response time start to start from client to server.
MF CS ART SS Sum X	Application response time, the summation X metric for exchange response time start to start from client to server.
MF SC ART SS N	Application response time, the n metric for exchange response time start to start from server to client.
MF SC ART SS Sum X	Application response time, the summation X metric for exchange response time start to start from server to client.
MF CS ART SE N	Application response time, the n metric for exchange response time start to end from client to server.
MF CS ART SE Sum X	Application response time, the summation X metric for exchange response time start to end from client to server.
MF SC ART SE N	Application response time, the n metric for exchange response time start to end from server to client.
MF SC ART SE Sum X	Application response time, the summation X metric for exchange response time start to end from server to client.
MF Conn Establish N	Connection Establishment, the n metric for connection establishment.
MF Conn Establish Sum X	Connection Establishment, the summation X for connection establishment.
MF Conn Graceful Term N	Connection Graceful Termination, the n metric for connection graceful termination.
MF Conn Graceful Term Sum X	Connection Graceful Termination, the summation X for connection graceful termination.

Field	Description
MF Conn Timeout Term N	Connection Timeout Termination, the n metric for connection timeout termination.
MF Conn Timeout Term Sum X	Connection Timeout Termination, the summation X for connection timeout termination.
MF CS Conn Retrans	Connection Retransmissions, the number of connection retransmissions from client to server.
MF SC Conn Retrans	Connection Retransmissions, the number of connection retransmissions from server to client.
MF CS Conn Out of Orders	Connection Out of Orders, the number of connection out of orders from client to server.
MF SC Conn Out of Orders	Connection Out of Orders, the number of connection out of orders from server to client.
MF Src MAC Address	Source MAC Address
MF Dst MAC Adress	Destination MAC Address
MF Probe ID	Unique identifier for the probe that generated the data.
MF Time Zone Bias From UTC	The difference in sconds between the local time zone and the UTC (GMT) time zone.
MF Day Light Saving Time Flag	True if it is day light savings time.
MF Local Standard Time Zone	Dependant upon location of CEM.
MF Local DST Time Zone	Dependant upon location of CEM.
MF Time Zone Code	
MF Response Time	Time between when the first HTTP request packet is sent and when the first response packet from the server is received.
MF Service Protocol	The network protocol of the flow.
MF URL Host	The hostname, if available, normalized to all lower-case.

Field	Description
MF URL Path	Path of the URL.
MF URL Domain	The domain (or “site”), derived from the hostname.
MF Timestamp Begin	Timestamp for when the flow has begun.
MF Timestamp Update	Timestamp for when the flow has been updated.
MF Timestamp End	Timestamp for when the flow has ended.
MF Service R1	First part on right of Data_Service.
MF Service R2	Second part on right of Data_Service.
MF Service R3	Third part on right of Data_Service.
MF Service R4	Fourth part on right of Data_Service.
MF Service R5	Fifth part on right of Data_Service.
MF Service R6	Sixth part on right of Data_Service.
MF Service R7	Seventh part on right of Data_Service.
MF Service R8	Eighth part on right of Data_Service.
MF Service R9	Ninth part on right of Data_Service.
MF Service R10	Tenth part on right of Data_Service.
MF Service R11	Eleventh part on right of Data_Service.
MF Service R12	Twelfth part on right of Data_Service.
MF URL Path Extension	Extension of the URL. (e.g. html).
MF Timestamp Local	Timestamp of the flow in local time.
MF Timestamp UTC	Timestamp of the flow in UTC (GMT) time.
MF Media Player	Establishes mapping for Media Player URL.
MF Media Type	Extracts Media Player URL.

Glossary

CEM: See Central Event Manager.

Central Event Manager (CEM): A component of XACCT*usage* that coordinates, manages, and controls the operation of the system.

Data Collection Module (DCM): (Formerly called Asynchronous Information Source Module.) A type of Information Source Module that provides data from the network elements, for example, the Check Point FireWall-1 ISM.

DCM: See Data Collection Module.

Data Enhancement Module (DEM): (Formerly called Synchronous Information Source Module.) A type of Information Source Module that enhances the data gathered from the network elements, for example, the DNS ISM.

DEM: See Data Enhancement Module.

Enhancement Procedure: The set of operations that define the route of the network session record from the Information Source that supplies the initial data (the trigger of the Enhancement Procedure) to the place where the data is stored (the target). The Enhancement Procedure includes Field Enhancements on every field of the target that receives information originating from the trigger.

Field Enhancement: Part of an Enhancement Procedure that defines how the data obtained from its trigger is used to fill a single field in the target.

Gatherer: A component of XACCT*usage* whose main function is to collect network traffic data from the Information Sources located on the network. The Gatherers defined are multi-threaded lightweight smart-agents designed to run on non-dedicated hosts as background processes.

Information Source (IS): 1. A network device or application server from which XACCT*usage* collects network session data. An Information Source can be a mail server, a firewall, a router, a DNS server, and the like. 2. An instance of an Information Source Module that is part of the XACCT*usage* configuration and hence is a system configuration object. For example, an Information Source of type DNS, called **dns-xacct**, which is part of the XACCT*usage* configuration and appears as an object in the XACCT tree.

Information Source Module (ISM): An add-on to XACCT*usage* whose function is to provide an interface between a Gatherer and a specific network element.

IP address: Internet Protocol address. A 4-byte address that uses numbers (rather than names) and uniquely identifies a host computer on the Internet, for example, **200.201.32.1**. The IP address can be split into a network number (or network address), a host number (a number unique to each host on the network), and sometimes also a sub-net mask.

IS: See Information Source.

ISM: See Information Source Module.

Unified Network Information Record (UNIR): A compact and efficient generic format in which network data is maintained and processed in XACCT*usage*.